

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

| | | |
|---------------------------|---|----------------------|
| UNITED STATES OF AMERICA, |) | |
| |) | |
| Plaintiff, |) | 18 CR 789 |
| |) | |
| vs. |) | Judge Gary Feinerman |
| |) | |
| DENY MITROVICH, |) | |
| |) | |
| Defendant. |) | |

MEMORANDUM OPINION AND ORDER

A grand jury charged Deny Mitrovich with knowingly possessing child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). Doc. 1. After denying Mitrovich’s motion to dismiss due to the Government’s alleged delay in obtaining an indictment, Doc. 32 (reported at 2019 WL 1773358 (N.D. Ill. Apr. 23, 2019)), the court granted Mitrovich’s motion to compel the Government to respond to two interrogatories, Docs. 72-73 (reported at 458 F. Supp. 3d 961 (N.D. Ill. 2020)). Dissatisfied with the Government’s efforts to comply with that order, Mitrovich moves the court to impose a discovery sanction, either in the form of the suppression of evidence or outright dismissal of the charges. Doc. 92 at 2. Mitrovich also argues that the Government’s failure to produce the evidence in question denies him his due process right to put on a defense and violates the Government’s duties under *Brady v. Maryland*, 373 U.S. 83 (1963). Doc. 92 at 15-26. The motion is denied.

Background

The relevant background is detailed in the opinion granting Mitrovich’s motion to compel. 458 F. Supp. 3d at 963-64. In short, law enforcement authorities in Australia and New Zealand clandestinely took control of a website called “The Love Zone,” which was known to

host child pornography. *Id.* at 963. The website was accessible only through the anonymizing web browser Tor, which hindered efforts to trace users' IP addresses. *Ibid.* The Oceanian authorities developed a workaround, though: they posted to the site a URL that linked to a child pornography video, but clicking the URL would start the download *outside* the Tor browser, allowing the user's IP address to be discovered. *Ibid.* Mitrovich clicked on the URL, revealing his true IP address. *Ibid.* Because the IP address was associated with an internet connection in the United States, the Oceanian authorities shared it with authorities in this country, who traced it to Mitrovich's residential address. *Ibid.* Federal law enforcement officers then obtained a warrant, searched Mitrovich's residence, and uncovered child pornography on his electronic devices. *Ibid.*

Mitrovich sought Criminal Rule 16 discovery from the Government concerning the technique used by the Oceanian authorities to uncover his IP address. *Id.* at 964. According to Mitrovich, that discovery would allow him to develop an argument that the technique constituted a Fourth Amendment search—one occurring without a warrant—and thus that all evidence attributable to the revealing of his IP address must be suppressed. *See ibid.* The Government objected to Mitrovich's discovery request as immaterial, so he moved to compel. *Ibid.* The key issue was whether Rule 16(a)(1)(E) required disclosure of the details of the unmasking technique. *Ibid.*; *see* Fed. R. Crim. P. 16(a)(1)(E)(i) (requiring the Government to produce evidence "within [its] possession, custody, or control" that "is material to preparing the defense").

Mitrovich's motion to compel turned on two questions. The first was "whether the investigative tools used to identify his IP address potentially effected a search within the meaning of the Fourth Amendment." 458 F. Supp. 3d at 964-65. The second was whether the

first question mattered for purposes of the exclusionary rule—that is, whether the Oceanian authorities’ conduct could be attributable to federal authorities in the United States, and thus be subject to the Fourth Amendment’s exclusionary rule, under the “joint venture” doctrine. *Ibid.*; *see id.* at 965 (“‘Evidence obtained in a search of an American citizen by foreign authorities operating within their own country is generally admissible in the courts of the United States even if the search does not otherwise comply with ... the Fourth Amendment.’ Under the joint venture doctrine, however, ‘if U.S. agents substantially participate in an extraterritorial search of a U.S. citizen and the foreign officials were essentially acting as agents for their American counterparts or the search amounted to a joint operation between American and foreign authorities, the Fourth Amendment generally applies.’”) (alteration in original) (citation omitted) (quoting *United States v. Stokes*, 726 F.3d 880, 890-91 (7th Cir. 2013)). As this court observed: “If the answer to either question is no, then any Fourth Amendment motion to suppress would be dead in the water, meaning that the discovery Mitrovich seeks would not be material, which in turn means that his motion must be denied. If the answer to both questions is yes, then the discovery is material and Mitrovich’s motion must be granted.” *Id.* at 965.

The court sided with Mitrovich, at least to the extent necessary to grant his motion. First, the court held that he “ha[d] made ‘at least a *prima facie* showing’ that the joint venture doctrine applies,” such that it could not reject outright the possibility that the exclusionary rule would require suppression of evidence obtained in a manner that violated the Fourth Amendment. *Id.* at 965-66 (quoting *United States v. Thompson*, 944 F.2d 1331, 1341 (7th Cir. 1991)). Second, the court held that Mitrovich “ha[d] made ‘at least a *prima facie* showing’ that malware was used to obtain his IP address” and that such use could qualify as a Fourth Amendment search. *Id.* at 967 (quoting *Thompson*, 944 F.2d at 1341). Given those showings, the court concluded that

Mitrovich's discovery requests were material to a potential Fourth Amendment suppression motion. It therefore ordered the Government to "produce discovery responsive to [the challenged interrogatories], subject to any targeted objections to the production of specific material." *Ibid.* The court concluded by noting the narrowness of its order: "By this ruling, the court holds only that Mitrovich has made a *prima facie* showing that the discovery is material to a Fourth Amendment motion to suppress that he might file; this ruling does not speak to the ultimate merits of any such motion." *Ibid.*

Long before Mitrovich's motion to compel, federal authorities sought to learn the technical details of the unmasking technique used by the Oceanian authorities. Doc. 96 at 8-13. But the information the federal authorities received was not of much use. In 2014, New Zealander authorities provided an "overview" of the technique but declined to "disclose the specific methodologies used." *Id.* at 11-12 (quoting emails from New Zealand law enforcement). Those authorities rebuffed attempts by federal authorities to follow up and learn more details. *Id.* at 12-13.

After the court's ruling, the Government renewed its efforts to obtain the pertinent software and/or source code from the Oceanian authorities. *Id.* at 13 n.6. Those efforts, too, were largely unsuccessful. While the Government obtained some vagaries about the technique from a former New Zealand law enforcement official, it was unable to obtain the details it sought, as New Zealander law barred him from disclosing those details. *Id.* at 13 & nn.5-6. So, while the Government has turned over everything in its possession relating to the technical details of how the Oceanian authorities identified Mitrovich's IP address, Doc. 92 at 3-6; Doc. 96 at 13, it has been unable to obtain the software and/or source code that would reveal precisely *how* the URL caused users' IP addresses to become unmasked, Doc. 96 at 13.

Discussion

Mitrovich views the Government's failure to turn over the requested software or source code as a violation of the court's ruling on his motion to compel, and therefore moves for discovery sanctions. *Id.* at 1, 8-15. Specifically, he asks that the court suppress all evidence that was obtained as a result of Mitrovich clicking on the URL or, in the alternative, dismiss the charges outright. *Id.* at 1, 9, 26-27. In addition, Mitrovich contends that the Government's failure to turn over the software or source code implicates his constitutional rights—either as a violation of his due process right to put on a defense, or of the Government's obligations under *Brady*. *Id.* at 15-26. The Government submits that it has satisfied its obligations under Rule 16, the court's discovery order, and the Constitution by turning over everything that it has and by making good faith (albeit unsuccessful) efforts to obtain more. Doc. 96.

I. Criminal Rule 16 and the Court's Discovery Order

Mitrovich first argues that sanctions are warranted because the Government, by failing to produce the software or source code used by the Oceanian authorities to reveal his IP address, flouted the court's order granting his motion to compel. Doc. 92 at 6-15. In so arguing, Mitrovich misunderstands the court's order.

To reiterate: The dispute giving rise to Mitrovich's motion to compel centered on two interrogatories Mitrovich served on the Government, each concerning the technique used by the Oceanian authorities to unmask his IP address. 458 F. Supp. 3d at 964. The Government objected, arguing that the discovery was not material to any Fourth Amendment challenge he might raise, either because the use of the Tor-evading URL did not constitute a Fourth Amendment search or because, even if it did, the resulting Fourth Amendment violation was committed by foreign authorities and thus could not be the basis for suppressing evidence. *Ibid.* The court rejected those arguments, holding that in order to obtain discovery, Mitrovich needed

only to make *prima facie* showings that there was a Fourth Amendment search and that federal law enforcement authorities' involvement in the Oceanian authorities' investigation was sufficient to implicate the exclusionary rule, and that he had made those showings. *Id.* at 965-67. In other words, the court held that the requested discovery *was* material within the meaning of Rule 16, and thus that the Government was obligated to substantively respond to the two interrogatories.

That was as far as the court went. The court did not, as Mitrovich suggests, order the Government to turn over any specific materials. *Id.* at 967 (“The Government shall produce discovery responsive to [the two] Requests ... , *subject to any targeted objections to the production of specific material.*”) (emphasis added). And had Mitrovich asked for such an order at the time, the court would have clarified then—as it clearly states now—that the Government has no obligation to turn over materials that it does not have and cannot obtain through good faith, diligent efforts. *See* Fed. R. Crim. P. 16 advisory committee’s note to 1966 amendment (“[T]he government’s obligation is limited to production of items within the possession, custody or control of the government, the existence of which is known, or by the exercise of due diligence may become known, to the attorney for the government.”). As the Rule itself puts it, the Government’s discovery obligation is to turn over materials that are “within [its] possession, custody, or control.” Fed. R. Crim. P. 16(a)(1)(E); *see United States v. Lee*, 723 F.3d 134, 141 (2d Cir. 2013) (explaining that the defendant was not entitled to the documents he sought “because these materials were not ... within the ‘government’s possession, custody, or control’”) (quoting Fed. R. Crim. P. 16(a)(1)(E)); *United States v. Dillow*, 980 F. Supp. 2d 879, 881-82 (N.D. Ohio 2013) (“[D]oes the ‘government’ have ‘custody’ in the Rule 16 sense of items apparently possessed only by a [different] law enforcement agency? ... [T]he weight of authority

... indicates the answer to that question is ‘No.’”) (citing *United States v. Marshall*, 132 F.3d 63, 68 (D.C. Cir. 1998); *United States v. Brazel*, 102 F.3d 1120, 1150 (11th Cir. 1997); and *United States v. Chavez-Vernaza*, 844 F.2d 1368, 1375 (9th Cir. 1987)). It follows that where the Government does not possess the requested materials but has tried diligently (though unsuccessfully) to obtain them, it has not violated Rule 16.

Mitrovich does not dispute that the Government has made efforts to learn additional details about the technique used by the Oceanian authorities to uncover his IP address, or that the Government has turned over everything it knows about that technique. Indeed, Mitrovich himself concedes that “[t]h[e] uncertain[t]y about the functionality of the hyperlink is shared by the government and FBI,” and that the Government has made efforts “to obtain more detailed information about the [Tor-evading] technique” from New Zealander law enforcement and from the former New Zealander official. Doc. 92 at 5 (quoting *id.* at 71). As far as the Government’s Rule 16 discovery obligations go, there is nothing left to be done. The Government must turn over what it possesses, but it cannot be faulted under Rule 16 for not turning over materials that it tried but was unable to obtain.

The court understands that, without the software or source code in hand, Mitrovich may find it difficult to mount a compelling Fourth Amendment suppression motion. But that is not the Government’s fault, and there is thus no legitimate basis for the Rule 16 discovery sanctions he seeks.

II. Due Process Right to Mount a Defense and *Brady*

The analysis differs somewhat when it comes to Mitrovich’s constitutional arguments. Mitrovich does not claim a due process right (beyond what Rule 16 provides) to obtain evidence that would assist him in pressing a Fourth Amendment motion to suppress, nor does he argue that the Government’s *Brady* duties extend to material relevant only to a Fourth Amendment

claim. Rather, Mitrovich’s due process arguments relate to his ability to defend against the charges on the merits. *Id.* at 13-15. And Mitrovich’s theory of why the software and source code are relevant to the merits appears to be this: He would admit at trial to clicking the URL, and would argue that doing so rendered his computer vulnerable to external attacks that caused child pornography to appear on his computer even though he never downloaded or knew about that material. *Id.* at 13-14 & nn.6-7.

Mitrovich first contends that without the source code, he is deprived of the opportunity to put on this defense, thereby rendering his prosecution fundamentally unfair, in violation of due process. Doc. 92 at 17-18; *see Fieldman v. Brannon*, 969 F.3d 792, 800 (7th Cir. 2020) (discussing a defendant’s due process “right to a ‘meaningful opportunity to present a complete defense’”) (quoting *Crane v. Kentucky*, 476 U.S. 683, 690 (1986)). That claim fails, even assuming those materials might provide some realistic avenue toward acquittal.

True enough, a criminal defendant has the right (whether grounded in the Fifth or Sixth Amendment) to put on a defense. *See Crane*, 476 U.S. at 690. But that does not mean that a constitutional violation occurs every time the Government prosecutes a defendant who is unable to obtain potentially exculpatory evidence. Sometimes, through nobody’s fault, evidence is simply unavailable—for example, the defendant’s lone alibi witness may die before giving a statement, or a video recording of the alleged crime may be accidentally deleted. As Mitrovich concedes, the unavailability of the evidence he seeks is not the Government’s fault, as the Oceanian authorities are simply unwilling to share it. There is thus no Government-imposed obstacle to Mitrovich’s ability to put on a defense, and therefore no violation of his due process right to put on a defense. Mitrovich’s argument is thus a mismatch for the due process right to put on a defense, and sounds more in the register of a *Brady* claim. It is the *Brady* right, also

sounding in due process, that provides that when the Government possesses exculpatory material, it must turn that material over to the defendant. *See United States v. Roberts*, 534 F.3d 560, 572 (7th Cir. 2008) (“Under *Brady*, the Government has the obligation to disclose any evidence in its possession that is both material and favorable to a defendant.”).

Mitrovich’s *Brady* argument, though, fails as well. Mitrovich has much to say about the importance of a prosecutor complying with her *Brady* obligations and how fundamental *Brady* is to a fair system of criminal justice. Doc. 92 at 18-20, 25-26. Those points are valid as far as they go, but Mitrovich overlooks the fact that a *Brady* duty arises only when the Government has in its possession “favorable” evidence, in the sense of being “either exculpatory or impeaching,” that is “material to the defense.” *United States v. King*, 910 F.3d 320, 326 (7th Cir. 2018) (Barrett, J.) (internal quotation marks omitted). It is the defendant’s burden to offer more than mere speculation that the undisclosed evidence in question is exculpatory and material. *See United States v. Morris*, 957 F.2d 1391, 1403 (7th Cir. 1992) (“Mere speculation that a government file may contain *Brady* material is not sufficient A due process standard which is satisfied by mere speculation would convert *Brady* into a discovery device and impose an undue burden upon the district court.”) (quoting *United States v. Navarro*, 737 F.2d 625, 631 (7th Cir. 1984)).

A logically anterior question is whether, for *Brady* purposes, the United States possesses the source code Mitrovich seeks. That question is more complicated than it appears, for the answer may turn on the extent to which the investigation that led to Mitrovich’s arrest was a joint one between federal and Oceanian authorities. *See United States v. Morris*, 80 F.3d 1151, 1169 (7th Cir. 1996) (explaining that the Government’s *Brady* duty to produce exculpatory evidence extends to “information possessed by other government agencies that have . . . involvement in the

investigation or prosecution at issue”). The parties seem to agree that the court would need an evidentiary hearing to make a finding on that front. Doc. 96 at 2; Doc. 97 at 14. For purposes of evaluating Mitrovich’s *Brady* claim, then, the court assumes without deciding that the United States constructively possesses the source code he seeks.

Mitrovich’s *Brady* argument still fails because he cannot offer anything more than speculation that the evidence in question is exculpatory. Mitrovich offers some technical authority suggesting that it is *possible* that when a person’s computer is infected with malware, other people may be able to store contraband on the computer’s drives without the owner’s knowledge. Doc. 92 at 14 nn.6-7. Yet he offers nothing even remotely suggesting that this might have happened here. Of course, the overview provided by the Oceanian authorities of its investigative techniques may be too vague to allow anyone—either the Government or Mitrovich’s expert—to understand every detail of how the URL worked. But that does not relieve Mitrovich of his burden to show that the evidence he seeks is exculpatory.

Mitrovich’s *Brady* argument also falters on the materiality prong. *Brady* requires the prosecution to turn over evidence only if it is “material,” meaning only if “there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different.” *United States v. Ballard*, 885 F.3d 500, 504 (7th Cir. 2018) (quoting *Turner v. United States*, 137 S. Ct. 1885, 1893 (2017)). By its terms, the materiality analysis assumes a post-“proceeding” vantage point, so it can be difficult for a defendant to demonstrate from an *ex ante* lens that a particular piece of evidence is material. *See United States v. Heine*, 314 F.R.D. 498, 503-04 (D. Or. 2016) (discussing the difficulty of conducting a *Brady* materiality analysis before trial); *United States v. Acosta*, 357 F. Supp. 3d 1228, 1233 (D. Nev. 2005) (noting that under the “cumulative ‘materiality’ standard” of *United States v. Bagley*, 473 U.S.


667 (1985), “it becomes extremely difficult if not impossible to discern before trial what combination of evidence will be deemed ‘material’ after trial under *Brady*”); *see also United States v. Pesaturo*, 519 F. Supp. 2d 177, 189 n.7 (D. Mass. 2007) (“Trial courts considering materiality under *Brady* have identified a difficulty applying [the materiality standard], crafted in the post-trial appellate context, to the pretrial discovery setting.”). The difficulty faced by Mitrovich is significantly exacerbated by the fancifulness of his proposed defense theory. It is hard to see how the evidence Mitrovich seeks could have any effect on a jury. So, to find materiality, the court would need to carefully evaluate the theory in light of all the evidence presented by the Government to support Mitrovich’s guilt.

The court cannot do that before trial. At this juncture, then, the court must turn away Mitrovich’s *Brady* claim, though he will of course be allowed to reassert it later in the case, assuming he can then also make a showing that the evidence is exculpatory. In so holding, the court does not suggest that a defendant can *never* lodge a successful *Brady* claim before trial, but only that it will generally be more difficult before trial for the defendant to show materiality, and that Mitrovich has failed to do so here. The court acknowledges and expresses its disagreement with *United States v. Safavian*, 233 F.R.D. 12, 16-17 (D.D.C. 2005), which suggests that a court can ignore materiality when a defendant presses a *Brady* claim before trial.

Conclusion

Mitrovich’s motion for discovery sanctions is denied.

July 7, 2021



United States District Judge